


[Web](#)
[Images](#)
[Groups](#)
[News](#)
[Froogle](#)
[more »](#)



[Advanced Search](#)
[Preferences](#)

WebResults 1 - 10 of about 123 for ID-NIKS. (0.45 seconds)Tip: Search for **English** results only. You can specify your search language in [Preferences](#)www.dj.kit.ac.jp/seminar/2000/abstract/ja/99630027-ja.txt

... 暗号技術の中で注目されているものの一つに個人識別情報
に基づく予備通信不要な鍵共有方式 (ID-NIKS) が挙げられる ...

2k - [Cached](#) - [Similar pages](#)<file:///X:/Plan/出張報告/平成11年度/暗号技術調査 ...>

... で開催され、約 50 名が全国から参加した。今回の特長
は、(1) ID - NIKS に関する発表が多かった、(2 ...

www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/SEC-199911.htm - 3k - [Cached](#) - [Similar pages](#)<file:///X:/Plan/出張報告/平成11年度/暗号技術調査 ...>

... 日立の推奨段数は 10 以上)。 — 以下はそ

... 其他の話題。 2 . ID - NIKS (ID Based Non Interactive Key ...

www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/SEC-199907.htm - 4k -
[Cached](#) - [Similar pages](#)

[More results from www.ipa.go.jp][United States Patent Application: 0020099941](#)

... [0006] ID-NIKS (ID-based Non-Interactive Key ... The ID-NIKS cryptosystem does not need
to exchange a public key and a secret key between the sender and receiver. ...

appft1.uspto.gov/.../email - 40k - [Supplemental Result](#) - [Cached](#) - [Similar pages](#)[\[PS\] 0E9fM""O@\\$H\\$=\\$!\\$r:Y\\$\(\\$kBe?t6J@~M""O@Bh](#)File Format: Adobe PostScript - [View as Text](#)

... ID ?pJs\$K4p\$E\$/806&M-J""!O (0J9. IDNIKS \$H5-=R\$9\$k) \$O!""?Mj\$N\$*\$1\$k%;%s%?\$r!MW\$H\$9\$sk\$,!" ... 2
%Z%"%j%\$s%0\$K4p\$E\$/ IDNIKS 2.1 %t%"%\$%f%Z%"%j%\$s%02CK!72. ...

www.ise.chuo-u.ac.jp/TISE/symp/2000/000831w/sakai.ps - [Similar pages](#)[Gamer.nl Forum - Planet Internet adsl comfort router instellingen](#)

... IP address: 10.0.0.138 My Subnet Mask: 255.255.255.0 Server IP Address: 0.0.0.0 PPTP

Account: mijn account password: mijn password Connection ID: Niks shit lukt ...

forum.gamers.nl/showthread.php?threadid=56444 - 38k - [Cached](#) - [Similar pages](#)[: TMF.be : We love Music](#)

... zeggen. Even hem corrigeren: Als je er last van heb ga naar kanaal
vip dat kanaal kunnen mensen zonder id niks zeggen. Arwenneke ...

www.tmf.be/index.php?page=forum&topic_id=8&thread_id=13205 - 47k - [Cached](#) - [Similar pages](#)[暗号入門 : CA,PKI,鍵共有とは ? | C4T](#)

... また、当社の「C4K」もこのDiffie-Hellman鍵共有法を利用し

て鍵を共有しています。 •ID-NIKS鍵共有 ID-NIKS (ID-based Non ...

c4t.jp/introduction/cryptography/cryptography07.html - 27k - Aug 7, 2004 - [Cached](#) - [Similar pages](#)

Best Available Copy

Bandwidth Market, Ltd

... [0007] A cryptosystem according to this technique (2) is called **ID-NIKS** (ID-based non-interactive key ... [0008] FIG. 1 shows principles for this **ID-NIKS** system. ...
www.bandwidthmarket.com/resources/patents/apps/2001/8/20010010724.html - 64k - Supplemental Result -
[Cached](#) - [Similar pages](#)

Universiteit Maastricht

Logo Universiteit Maastricht. dit deel hele site. ...
www.unimaas.nl/.../nieuws.htm&fac=um%20Algemeen&nid=70OG00IVK4FQVBU5AN6W&id=niks&taal=nl - 10k
- Aug 7, 2004 - [Cached](#) - [Similar pages](#)

Goooooogle ►

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [Next](#)[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google

Best Available Copy

IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE


[Membership](#) | [Publications/Services](#) | [Standards](#) | [Conferences](#) | [Careers/Jobs](#)
IEEE Xplore
RELEASE 1.2

 Welcome
 United States Patent and Trademark Office

[Help](#) | [FAQ](#) | [Terms](#) | [IEEE Peer Review](#)
[Quick Links](#)

» See

Welcome to IEEE Xplore

- ☐ Home
- ☐ What Can I Access?
- ☐ Log-out

Tables of Contents

- ☐ Journals & Magazines
- ☐ Conference Proceedings
- ☐ Standards

Search

- ☐ By Author
- ☐ Basic
- ☐ Advanced

Member Services

- ☐ Join IEEE
- ☐ Establish IEEE Web Account
- ☐ Access the IEEE Member Digital Library

IEEE Enterprise

- ☐ Access the IEEE Enterprise File Cabinet

 Your search matched **2** of **1058483** documents.

 A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Refine This Search:

You may refine your search by editing the current search expression or enter a new one in the text box.

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

1 Collusion attack free identity-based cryptosystems
Tanaka, H.;

Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on , 2002

Pages:411

[\[Abstract\]](#)
[\[PDF Full-Text \(225 KB\)\]](#)
IEEE CNF
2 Identity-based non-interactive key sharing equivalent to RSA public cryptosystem
Tanaka, H.;

Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on , 16-21 Aug. 1998

Pages:384

[\[Abstract\]](#)
[\[PDF Full-Text \(84 KB\)\]](#)
IEEE CNF

Print Format

[Home](#) | [Log-out](#) | [Journals](#) | [Conference Proceedings](#) | [Standards](#) | [Search by Author](#) | [Basic Search](#) | [Advanced Search](#) | [Join IEEE](#) | [Web Account](#) | [New this week](#) | [OPAC Linking Information](#) | [Your Feedback](#) | [Technical Support](#) | [Email Alerting](#) | [No Robots Please](#) | [Release Notes](#) | [IEEE Online Publications](#) | [Help](#) | [FAQ](#) | [Terms](#) | [Back to Top](#)

Copyright © 2004 IEEE — All rights reserved

Best Available Copy



US Patent & Trademark Office

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide



THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Published since January 1947 and Published before February 2000

Terms used **identity based**

Found 2 of 100,313

Sort results by

Display results

[Save results to a Binder](#)[Search Tips](#)
☐ Open results in a new window
[Try an Advanced Search](#)[Try this search in The ACM Guide](#)

Results 1 - 2 of 2

Relevance scale ☐ ☐ ☐ ☐ ☐

1 Authentication primitives and their compilation

Martín Abadi, Cédric Fournet, Georges Gonthier

 January 2000 **Proceedings of the 27th ACM SIGPLAN-SIGACT symposium on Principles of programming languages**

Full text available: pdf(1.55 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Adopting a programming-language perspective, we study the problem of implementing authentication in a distributed system. We define a process calculus with constructs for authentication and show how this calculus can be translated to a lower-level language using marshaling, multiplexing, and cryptographic protocols. Authentication serves for identity-based security in the source language and enables simplifications in the translation. We reason about correctness relying on the concepts of o ...

2 Authentication in distributed systems: theory and practice

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber

November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4

Full text available: pdf(3.37 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegated authority. The theory shows how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We ...

Keywords: certification authority, delegation, group, interprocess communication, key distribution, loading programs, path name, principal, role, secure channel, speaks for, trusted computing base

Rest Available Copy

Results 1 - 2 of 2

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:

[Adobe Acrobat](#)[QuickTime](#)[Windows Media Player](#)[Real Player](#)